Kentucky Board of Elections Privacy and Security Report – Suitable for Public Discussion

December 20, 2018

7580 N Dobson Road, Suite 201
Scottsdale, AZ 85256

888.682.5911
www.CyberScout.com

Scottsdale, AZ / Providence, RI / New York, NY
Montreal, Canada / Galway, Ireland

Contents

Overview

This report summarizes CyberScout's Election Security Assessment for the Commonwealth of Kentucky at the request of the Secretary of State and Chief Election Official ("Secretary of State/Chief Election Official") and the Kentucky State Board of Elections to ensure the continued integrity of the Commonwealth's elections. CyberScout spent eleven months reviewing and observing the practices, technology, organizational controls, and documentation related to the protection and conduct of elections in Kentucky.

We visited seven counties, observing a special election in Crittenden County, and we spent more than 650 man-hours with the State Board of Elections' engineers and managers, the Commonwealth Office of Technology, members of the Secretary of State's office, and members of the Board. We made 15 trips to Frankfort and various counties, and we performed technical analysis of dozens of systems related to technology.

CyberScout Qualifications

Prior to beginning this effort, our team's voting infrastructure expert, Harri Hursti, had deep experience with the voting infrastructure that the Commonwealth of Kentucky uses, conducting penetration testing, vulnerability assessments, and process analyses of the real-world deployments of these devices in other states. Mr. Hursti is one of the most highly regarded consultants in the world in the field of detecting security vulnerabilities in the voting machines and systems that are in use across the Commonwealth of Kentucky.

Our extensive experience in protecting the identity of individuals (we have worked with thousands of organizations in the public and private sectors) proved helpful in understanding risks posed to voters' privacy. Shortly before this engagement, the team was involved in protecting voter privacy in Ohio and California during recent elections by deploying a combination of process, technology and awareness to choose the best methods for ensuring privacy.

Our team has conducted audits in a number of states, including Ohio and California, for prior elections, and given expert testimony as voting machine security experts in states where recounts were either considered or conducted after the 2016 Presidential election, including Michigan and Wisconsin.

Our experience allowed us to provide consistency and continuity across the full scope of the project. Using a single team for all four of the interconnected objectives has allowed the Kentucky Board of Elections to receive the best possible advice from beginning to end. For example, risks identified during the identity protection and voter security phases informed decisions that were made later in the year, as the Kentucky Board of Elections rolls out new initiatives, like ePollBooks and cloud services.

Objectives for the Assessment

Our assessment was divided into four objectives, designed to address the areas of greatest risk to the security of a state's election process:

> ***Objective 1***: Determining and mitigating the risks in how the Kentucky State Board of Elections protects the identities of its registered voters.
>
> ***Objective 2***: Identifying and recommending actions to mitigate the shortcomings in the security of the voting process
>
> ***Objective 3***: Reviewing whether the data integrity and attribution of votes is good enough that the risk of inaccuracy in post-election recounts and audits will be limited
>
> ***Objective 4***: Advising the Kentucky State Board of Elections on security and privacy risks inherent in its new voter-related initiatives as they are deployed in 2017

This report will address the opportunities for improvement in each category, but there are systemic conclusions to be drawn, as well.

General Findings

In general, we found resistance and apprehension within SBE to the Secretary of State/Chief Election Official's goal to assess the security and privacy of the Voter Registration System and the proliferation of election processes and standards. Alignment between these different agencies is key to making sure that Kentucky is focusing on defending its election process against adversaries; there is room for improvement in that regard.

We also saw opportunities for improvement in Kentucky's vulnerability management program. There are many effective controls, including COT's assessments of its infrastructure, the Department of Homeland Security's scans, and SBE's own reviews, but these efforts are piecemeal. There needs to be an overarching approach that considers all the different ways an adversary could influence an election. For example, initial efforts to select an ePollbooks vendor were not coordinated with respect to how secure these systems could be or how resilient they may be. The first approach to selecting an ePollbooks vendor focused on making sure the ePollbooks worked well were able to transfer data as needed. CyberScout assisted in making sure that the security and privacy of the ePollbooks were also considered in the selection process. Without this involvement, the ability of the ePollbooks to keep data confidential or to restrict access to authorized individuals was not in the plan for consideration during vendor selection.

We saw opportunities for improvement in understanding what attack vectors could be effectively used by an adversary. A more collaborative approach between agencies could help.

Important Note

The recommendations made in the confidential report, many of which are reflected here, reflect a point in time. Many of these issues have been addressed or are being addressed by December 2018, so some of the recommendations have already been implemented.

Executive Summary – Objective 1 – Voter Registration System

Our approach included several visits to COT and SBE facilities, interviews with key personnel at both organizations, and technical testing in the form of vulnerability assessment and penetration testing of the Voter Registration System components. We also reviewed the artifacts from other vulnerability assessments and penetration tests performed by the Department of Homeland Security.

CyberScout has identified many practices and activities that the Commonwealth can be proud of. SBE and COT have collaborated to effectively protect voter information and the voting process to date, even as other states have experienced breaches and incursions. Both groups have deep expertise and individuals who are dedicated to maintaining the integrity and security of the election process. It was clear from our visit that the systems engineers and managers in both groups feel a serious sense of responsibility for protecting the vote.

The technical defenses, particularly those that protect the perimeter of the network and those that protect the Voter Registration servers, appear to be very effective. The state has created a “defense in depth” approach that makes it difficult to directly penetrate the key systems from outside the network. Regular testing and review of these technical defenses provides assurance that the Voter Registration System is well-protected.

Our most important recommendations for making sure that voter rolls remain secure have to do with process and communication between COT, SBE, and other stakeholders. In order of priority, we recommend that the Commonwealth address these issues:

1. *Detective Controls.*

   It is important to have effective detective controls in place, so that COT, SBE, and the Secretary of State/Chief Election Official have the evidence available to determine whether someone used unauthorized permission to change voter data. Without this kind of control in place, it would be possible for someone to gain permission to make changes to the data, effect those changes, and then cover their tracks by changing their permissions back to an inconspicuous configuration.

   We recommend that SBE, COT, and the Secretary of State/Chief Election Official collaborate to test detective controls as capabilities are added and deploy the capability in combination with an audit process that will periodically review the permission changes.

2. *Ensure consistent security controls at localities across Kentucky.*

   During our visits to various locations across the Commonwealth, we saw an opportunity to enforce consistent security and privacy controls. In theory, some of these locations, if penetrated, could represent a path to other sensitive data.

   We recommend that the Secretary of State/Chief of Election Official institute a program of vulnerability management for the localities, including these measures:

   - Education and awareness for the local officials including wireless networking security, physical security, good practices for physically securing networked devices, and good practices for password management.
   - Conduct vulnerability management measures consistent with NIST 800-53 and NIST Critical Infrastructure guidelines. These can be performed with little overhead, using readily available tools, or the Commonwealth could appeal to the Federal Government for support.

3. *Report complete results of vulnerability management activities and threats to all stakeholders, including COT, SBE, and the Secretary of State/Chief Election Official.*

   A risk exists that COT vulnerability management information is not thoroughly shared between the key groups (COT, the Secretary of State's office, and SBE). This can lead to challenges in categorizing the importance of the vulnerabilities, as COT is less informed about potential consequences of breaches than SBE would be. This also leads to a situation where accountability is more challenging than it needs to be and longer-term planning of security investments may be affected.

   We recommend that SBE execute its plans to implement three steps:

   - Enter into an arrangement with a vulnerability management third party (this is currently planned) which will report vulnerabilities in real time directly to SBE.
   - Have SBE enter into a collaboration with the Multi-State Information Sharing and Analysis Center (MS-ISAC) in order to learn what other states are doing and to keep apprised of the latest threats to voter rolls. This will provide good threat intelligence and will promote collaborative ideas

   We also recommend that SBE develop a formal process for reporting important findings and activities to COT. SBE and COT should determine together what information would be useful for COT to stay apprised of. SBE shall also report a

summary of vulnerabilities and the plans to mitigate those vulnerabilities to the Secretary of State/Chief Election Official, so that he or she can ensure that the risks are being addresses and so that he or she can report on these efforts to the citizens of Kentucky when appropriate.

4. *Develop one repeatable, cohesive security auditing plan for VRS*

   The VRS and its associated systems are not part of a formal internal controls and oversight program that occurs on a regular basis. There are elements of such a program included in the vulnerability management program, Business Continuity Planning, and daily maintenance, and these elements can form the basis of a security risk management plan for the voter registration data. This will ensure that all security risks are considered and evaluated and that continuous improvement or the processes, technologies, and governance can occur.

   The results of this effort should be shared between COT, SBE, and the Secretary of State/Chief Election Official, and plans for improvement should be tracked carefully. Irregularities should be logged and sent to the COT and Secretary of State on a daily basis.

5. *Ensure all potential attack vectors are included in technical testing*

   There is a risk that some indirect attack vectors may not be included in vulnerability testing. We recommend that COT and SBE collaborate to establishing a process for identifying threats to the Voter Registration System.

   Ensuring that not only the VRS is secure, but that the systems that can be used to “hop” to the VRS are also secure, will provide a more complete picture about the likelihood and severity of the threat.

The risks identified in Kentucky are typical of what might be found in a relatively secure system. The vulnerabilities discovered are all categorized as “low” risk according to the Common Vulnerability Scoring System (“CVSS”), as published by the National Infrastructure Advisory Council.

We also note that Kentucky has acted on the recommendation of developing knowledge-sharing partnerships with other government resources by becoming participants in the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), as well as it’s predecessor, the MS-ISAC, as well as actively participating in national conferences for Secretaries of State and State Election Directors.

The fact that Kentucky was not among the group of 21 states that were probed or attacked in the last election further bolsters this perspective. However, CyberScout observed some processes that could be improved within the organizations.

CyberScout also conducted an architecture review and examination of the network that includes the Voter Registration System.

We began with a visit to the facility where the architecture resides. We noted that physical security measures were sound.
Overall, physical security of the network was outstanding. We examined the components of the network and verified through observation that the components were configured as described by the COT Engineer.

Overall, we found no recommendations for improvement in the physical security or in the design or implementation of the network. COT personnel were generally knowledgeable, and COT governance was through, as indicated in our interviews with the Chief Information Security Officer.

Executive Summary – Objective 2 – Voting Process and Technology

We visited seven counties and observed a live voting event in one county. We found that the county clerks and their staffs were well-informed about the procedures that are in place to prevent security breaches in their systems. Each of them had resources to rely upon when they had questions, and each of them understood the importance of measures like tamper-proofing and zeroizing machines before and after an election.

The challenge that Kentucky faces is that there are vulnerabilities inherent in the voting machines and the voting infrastructure, and many of these vulnerabilities have no technical fix that the Commonwealth can put into place. This means that the Secretary of State/Chief Election Official, the county clerks and their staffs need to undertake compensating steps to try to ensure that the vulnerabilities are not exploited.

First, the Commonwealth can address some general risks through strong governance and strategy. Key recommendations in this category include:

1. Requiring voting machine vendors to report on the shortcomings and potential compensating controls found in their systems using a methodology for risk assessment that is consistent with NIST Critical Infrastructure Standards.
2. Developing a process where the contractors who support the voting infrastructure are closely coordinated with the voting machine manufacturers, so that the contractors can effectively mitigate risks that are inherent in the systems.
3. Review and improve the education and awareness processes for county clerks.

Next, the Commonwealth can require that its vendors address some of the riskier vulnerabilities in their systems. These are described in the confidential report, but not in this document.

Finally, the Commonwealth should put some practices into place for SBE and those who support elections across Kentucky to include education and awareness, tamper-proofing measures, and processes that improve consistent preventative and detective measures.

Executive Summary – Objective 3 – Reliability of the Count

SBE and COT have collaborated to effectively protect voter information and the voting process to date, even as other states have experienced breaches and incursions. Both groups have expertise in fraud detection and monitoring, even if the latest techniques (like Risk Limiting Audits) are not fully implemented in Kentucky.

During our observation of a voting event in one of the counties and our visits to six other counties, as well as our observations at SBE in Frankfort, we saw that the laws and guidance regarding the auditing and fraud detection in the voting infrastructure have been deployed effectively. Compared to many other states, Kentucky is diligent, thorough, and proactive in trying to ensure its elections are safe and accurate.

There is still room for improvement, however. Many of the auditing and fraud detection risks that Kentucky faces are the result of challenges in securing voting machines and issues in integrating a process improvement program across all stakeholders in the state.

In Reviewing whether the data integrity and attribution of votes is good enough that the risk of inaccuracy in post-election recounts and audits will be limited, our general recommendations for improving fraud detection and auditing can be summarized in three categories.

1. Committing to a risk-based audit process that is appropriate to Kentucky's mix of DREs with Voter Verified Paper Audit Trails and those without.
2. Establishing oversight and direct visibility into the audit processes of voting machine vendors.
3. More carefully controlling the activities of voting machine contractors and vendors.

Our recommendations for improving the auditing and fraud-detection process, include:

1. Develop controls to oversee the vendors for Kentucky's voting machines. A representative of the State Board of Elections should review and spot-check activity related to the management of the storage devices by those vendors. The vendors should certify adherence with appropriate measures when handling or accessing the storage devices.

2. Physical security for the voting machines and equipment between election days should adhere to a standard that includes preventative controls (locks and observation of the area), as well as detective controls (tamper proof seals on doors or electronic surveillance).

3. Consider implementing Risk Limiting Audit methods to sample vote counts at polling locations and compare them with results on voting day. These methods are being adopted by other states and provide faster and more thorough fraud detection measures than Kentucky is currently following.

Executive Summary – Objective 4 – Transition of Security Controls to Future State

During our analysis, it was clear that there is thorough process in place and guidance to limit the exposure of the machines. SBE has deep expertise in its engineering group.

This objective included a definition of current controls for the systems that are critical to elections and a mapping of future controls after the Azure Cloud and ePollbooks are implemented.

The matrix below offers a sample of key controls that will be affected during the transition to the future state. We have not included other important controls in this document, due to the sensitivity of the issues; they are included in the confidential report.

We have considered the risks involved in transitioning these controls, and we identify that these risks should be addressed:

Issue	Risk	Recommendation
The asset inventory will change to the point where tracking equipment will present a new challenge. Thousands of new devices (ePollbooks) will be added to the inventory and dispersed through the state.	ePollbooks systems have been compromised in other states during the last year. If an adversary were to obtain one of the devices, there is a risk that it could be used as an attack vector to alter voter registration information, disrupting accurate voting on election day.	The ePollbook devices should be inventoried and their location tracked. Current barcoding systems are in use for some of the elections infrastructure. This same system could be used to check devices into and out of locations before and after election day. There will be a new manual process of adding and removing these devices from the inventory and reviewing the inventory on a regular basis. This duty should be assigned to a vetted contractor or to an additional member of the

Issue	Risk	Recommendation
		SBE staff, but additional budget may be needed.
Presently, SBE is challenged to complete all required county clerk training with the available human resources available to perform the training as required by KAR 6:040.	The most important defense to unknown threats is a vigilant team of county clerks and staffs on the ground in the precincts at the county offices. If these people are not prepared to notice threats, they are less likely to prevent or detect them.	Hire or contract to train County Clerks and their staffs in a manner that ensures they are prepared. Implement post-training testing concerning processes and threats to gauge preparedness.
SBE staff leverage their experience and judgement to sustain compliance with de facto information security roles and responsibilities, which have evolved over time, related to internal staff roles and external partners involvement in SBE processes.	Without a proper definition of roles and responsibilities, it is unlikely that all Counties will have appropriately qualified individuals taking care of security controls on or before election day.	Codify roles and responsibilities for different classifications of counties and communicate how County Clerks can comply with these roles and responsibilities.
While the capability exists to restore the VRS to a particular recovery point, no “rollback” capability is built into the database.	In the event of an outage or a breach that alters the data in the VRS, it may be difficult to implement the “last known good” version of the VRS database. This could prevent reliable recovery.	Include rollback capabilities and processes in the next version of the VRS.